IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1.   (Currently Amended) A method for automated adaptive reprovisioning of servers under security assault, the method comprising:

detecting a security assault or a possible security assault on a first server;

incrementing a counter that tracks a total number of times that the first server has been victim of a security assault or a possible security assault;

notifying a human operator if a value of said counter exceeds a maximum limit;

and

reprovisioning by automatically creating a new server instance with a new server configuration to perform at least one of the tasks performed by said first server, if said value of said counter does not exceed the maximum limit, wherein said new server configuration for said new server instance is selected from a table comprising a plurality of new server configurations, said new server configuration being associated in said table with said value of said counter such that a particular configuration of said new server configuration depends on the total number of times that said first server has been victim of a _different_ security assault or a _different_ possible security assault.

2.   (Original) The method of claim 1, wherein said detecting comprises determining if said first server is a candidate for reprovisioning, because of properties or behavior that suggest its security has been compromised or is likely to be compromised, or its functioning otherwise unacceptably impaired, by a security assault.

3.   (Original)   The method of claim 1, wherein said reprovisioning comprises automatically bringing up said new server instance, or otherwise making available said new server instance to customers or other users of said first server.

4.   (Original)   The method of claim 1, further comprising bringing down said first server prior to said reprovisioning.

5.   (Original)   The method of claim 1, wherein said new server instance brought up in said reprovisioning differs from said first server in at least one parameter.

6.   (Original)   The method of claim 1, wherein a difference between said new server instance and said first server is responsive to whether or not other security incidents have been detected in a network to which said servers are coupled.

7.   (Previously Presented)   The method of claim 1, wherein a difference between said new server instance and said first server is responsive to a nature of any other security incidents that have been detected in a network to which said servers are coupled.

8.   (Original)   The method of claim 1, wherein a difference between said new server instance and said first server is responsive to a probable compromise or a functional impairment observed in said detection.

9.   (Original) The method of claim 1, wherein a difference between said new server instance and said first server includes a version of server software used by said servers.

10.   (Original) The method of claim 1, wherein a difference between said new server instance and said first server includes a version of operating system software used by said servers.

11.   (Original) The method of claim 1, wherein a difference between said new server instance and said first server includes a version of network connectivity software used by said servers.

12.   (Previously Presented) The method of claim 1, wherein a difference between said new server instance and said first server includes a strength of encryption used by said servers.

13.   (Original) The method of claim 1, wherein a difference between said new server instance and said first server includes a degree of function offered to users by said servers.

14.   (Original) The method of claim 1, wherein said new server instance brought up in said reprovisioning differs from said first server only if more than a fixed number of instances of probable server compromise have been observed.

15.   (Original) The method of claim 1, wherein a difference between said new server instance and said first server is responsive to a number of probable server compromises that have been observed.

16.   (Previously Presented)   The method of claim 1, wherein said first server comprises a computer providing services through a network.

17.   (Previously Presented)   The method of claim 1, wherein said first server comprises a program running on a network-coupled computer, providing services through a network.

18. – 30.   (Cancelled)